Visa Request System (VRS)

Privacy Impact Assessment

1. Contact Information

Department of State Privacy Coordinator
Margaret P. Grafeld
Bureau of Administration
Global Information Services
Office of Information Programs and Services

2. System Information

(a) Date PIA was completed: September 26, 2012

(b) Name of system: Visa Request System

(c) System acronym: VRS

(d) IT Asset Baseline (ITAB) number: 4391

(e) System description:

In addition to producing diplomatic, official and no-fee passports for all government agencies, CA/PPT's Special Issuance Agency (SIA) both obtains and facilitates visas for official U.S. government travel from foreign embassies and/or consulates. In all cases SIA uses Visa Request System (VRS) to generate a formal letter to the foreign embassy/consulate requesting the issuance of a diplomatic or official visa. In some cases, SIA provides the letter to the employing agency which interacts with the Embassy itself. In other cases, SIA submits the complete visa application package, including the visa request letter, directly to the foreign embassy/consulate. As part of the process, SIA uses VRS to track and monitor the letters and visa applications sent to and collected from the respective foreign embassies/consulates.

(f) Reason for performing PIA:

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(g) Explanation of modification (if applicable): Moving system from SQL to Oracle

(h) Date of previous PIA (if applicable): 10/20/2009

3. Characterization of the Information

The system:

☐ does NOT contain PII. If this is the case, you must only complete Section 13.

☒ does contain PII. If this is the case, you must complete the entire template.

a. What elements of PII are collected and maintained by the system? What are the sources of the information?

Personally identifiable information (PII) that is contained includes: full name, date of birth, place of birth, gender, photograph, and a passport number.

The sources of information for VRS are U.S. government agencies and their employees when the employees need to apply for a foreign diplomatic or official visa for official United State Government (USG) travel.

b. How is the information collected?

The data in VRS is collected from a combination of 1) the traveler's diplomatic or official passport, 2) U.S. government travel orders and/or an official memorandum from the traveler's employing agency, and/or 3) country-specific visa applications completed by the traveler or the employing agency.

All foreign visa requests processed through this system require official notification from the State Department that the traveler/employee is going on official travel to represent the U.S. government. This notification is created through VRS. VRS is used to generate cover letters that accompany visa request packages. A hard copy package is comprised of the passport, visa form, photos, and any supplemental forms the host country may require. The package is then delivered to the foreign embassy.

The number of days required to process a visa request by a foreign embassy varies. The majority of the embassies do not contact SIA when a visa is ready. After a courier delivers a package to a foreign embassy for processing, the courier returns after the specified time frame required to process the visa package and tries to retrieve the passport with the visas. If the package has not been processed, the VRS personnel will reschedule pick-up when completed.

c. Why is the information collected and maintained?

The information is collected and maintained to produce official correspondence from the Department of State to a foreign embassy or consulate requesting the issuance of a diplomatic or official visa to an individual traveling abroad on U.S. government business. The information is also used to track and monitor the status of visa applications pending action by foreign embassies. Each element of PII collected is required to obtain a foreign visa for official travel.

d. How will the information be checked for accuracy?

The data received from applicants on the application is verified primarily by a manual review and comparison of the information on 1) the traveler's diplomatic or official passport, 2) the U.S. government travel orders and/or an official memorandum from the traveler's employing agency, and/or 3) country-specific visa applications completed by the traveler or the employing agency.

e. What specific legal authorities, arrangements, and/or agreements define the collection of information?

- 22 U.S.C. 3904 (Functions of the Foreign Service, including protection of U.S. citizens in foreign countries under the Vienna Convention on Consular Relations and assistance to other agencies)
- 22 U.S.C. 1731 (Protection of naturalized U.S. citizens in foreign countries)

f. Privacy Impact Analysis: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is a privacy risk of collecting more information about visa applicants than is necessary to accomplish the purposes of the VRS program. This risk has been mitigated by CA practice of collecting only a limited amount of information about individual, as it is required to adjudicate the Visa process. The privacy risk of incorrect data attributed to an individual visa applicant is mitigated by the manual review of information, which is obtained for the individuals employing agency.

4. Uses of the Information

a. Describe all uses of the information.

The Department of State uses the information to generate letters addressed to foreign embassies, and to track and monitor requests to foreign embassies to issue visas to personnel traveling on behalf of the U.S. Government. The data collected from the applicant in the VRS database is the minimum amount of PII necessary to produce the required documentation for a foreign embassy or consulate to issue a visa.

b. What types of methods are used to analyze the data? What new information may be produced?

VRS data is used to generate information on patterns of delays and denials by foreign governments in issuance of official or diplomatic visas to personnel traveling on U.S. government business.

c. If the system uses commercial information, publicly available information, or information from other Federal agency databases, explain how it is used.

VRS does not use any commercial information, publicly available information, or information from any other Federal agency database.

d. Are contractors involved in the uses of the PII?

VRS is a government off-the-shelf (GOTS) product owned by CA/CST that has both contractor and government users. The development and maintenance of VRS is performed by contractor personnel of URS-Apptis, under direction of CA/CST, located at:

6430 Rockledge Drive
Suite 600
Bethesda, MD 20817

e. Privacy Impact Analysis: Describe the types of controls that may be in place to ensure that information is handled in accordance with the above uses.

User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance. The identity of individuals is verified when they log into this Active Directory (AD) account. The AD account credentials are forwarded on to VRS upon going to the webpage and matching the account to the VRS user database table. Mandatory annual security/privacy training is required for all authorized users including security training and regular refreshment training.

All users, including external Agency users, are screened prior to their employment with the Department or their respective Agency. The Bureau of Diplomatic Security is responsible for the investigations of personnel in conjunction with normal hiring practices. This investigation consists of a review of a completed security questionnaire, a name check against applicable government, police, credit and fingerprint records, and may include a personal interview if warranted. In addition, before given access to the OpenNet and any CA/CST system, including VRS, users are required to sign non-disclosure agreements, acceptable use agreements, conflict-of-interest agreements, and rules of behavior agreements.

Consular post officers/users, system administrators, and database administrators are trained through the security awareness training to safeguard PII from unauthorized users by storing diskettes, CDs, and printouts in a safe and secure manner. Shredders and/or burn boxes are provided throughout the post and domestic sites and external agencies for the proper disposal of paper that contains PII.

5. Retention

a. How long is information retained?

Per the Department of State's Domestic Records Disposition Schedules, Chapter 13: Passport Records, A-13-002-06 Visa Request System, records within the Visa Request System are used to track and monitor the application process of obtaining visas from foreign embassies and/or consulates for official U.S. government travelers.

Active records must be destroyed five (5) years after issuance. (DispAuthNo: N1-059-09-25, item 1a.)

Paper records produced by this application are shredded or burned, per internal Department of State requirements for handling visas and Department of State record disposition schedules.

b. Privacy Impact Analysis: Discuss the risks associated with the duration that data is retained and how those risks are mitigated.

Records retention bears on privacy risk in two ways. First, the longer the records exist, the greater they are at risk to unauthorized use or exposure. Second, the longer records exist, the more likely inaccuracies will develop as a consequence of aging.

All physical records containing PII are maintained in secured file cabinets or in restricted areas, to which access is limited to authorized personnel only. Access to computerized files is password-protected and under the direct supervision of the system manager. When records have reached their retention end-date, they are immediately retired or destroyed in accordance with the National Archive and Records Administration (NARA) rules.

Since the Visa Request System contains sensitive personally identifiable information, such as passport number combined with date of birth, the data maintained by VRS is destroyed after a 5 year period to ensure that the data is not used for unauthorized purposes and reduce the risk of data breach.

Information is shared by secure transmission methods permitted under the Department of State policy for the handling and transmission of sensitive but unclassified (SBU) information. VRS backup information is protected from unauthorized modification by the physical security and access controls in place at PPT/SIA. VRS data is stored on site in a locked server room with cipher lock. Only cleared technical personnel (government and contractors) are allowed to access the server room housing VRS servers, and no one is allowed to access the system until the appropriate background screening has been completed.

6. Internal Sharing and Disclosure

a. With which internal organizations is the information shared? What information is shared? For what purpose is the information shared?

This information is not shared with any internal organizations.

b. How is the information transmitted or disclosed? What safeguards are in place for each sharing arrangement?

Information is not shared internally.

c. Privacy Impact Analysis: Describe risks to privacy from internal sharing and disclosure and describe how the risks are mitigated.

No information is shared internally.

7. External Sharing and Disclosure

a. With which external organizations is the information shared? What information is shared? For what purpose is the information shared?

The completed Visa package is delivered to the foreign embassies and/or consulates. No other external organizations receive information from VRS.

b. How is the information shared outside the Department? What safeguards are in place for each sharing arrangement?

The information is shared only via a paper package delivered to the foreign embassies and/or consulates.

c. Privacy Impact Analysis: Describe risks to privacy from external sharing and disclosure and describe how the risks are mitigated.

The risk is minimized by only sharing a paper copy of the package with the embassy foreign embassies and/or consulates. This reduces the risk of unauthorized access by individuals who are not part of the Visa process.

Residual risk is accepted through the authorization process.

8. Notice

The system:

☒ constitutes a system of records covered by the Privacy Act.

Provide number and name of each applicable systems of records:

- Visa Records. STATE-39
- Passport Records. STATE-26

□ does not constitute a system of records covered by the Privacy Act.

a. Is notice provided to the individual prior to collection of their information?

Notice of the purpose, use and authority for collection of information submitted is described in the System of Records Notices titled STATE-39, Visa Records, and STATE-26, Passport Records.

b. Do individuals have the opportunity and/or right to decline to provide information?

Yes, an individual does have the opportunity or right to decline to provide information. However, if he or she declines, he or she will not be provided with the administrative service he or she is requesting (i.e. assistance in obtaining a foreign visa).

c. Do individuals have the right to consent to limited, special, and/or specific uses of the information? If so, how does the individual exercise the right?

No. The information is used only for the purpose of requesting and tracking the visa. No other uses are provided for VRS.

d. Privacy Impact Analysis: Describe how notice is provided to individuals and how the risks associated with individuals being unaware of the collection are mitigated.

By providing the notice through the SORNs, which are published both in the *Federal Register* and the Departments' webpage, notice is provided to the individual in multiple places. As these locations are readily available to the public, this mitigates the risk that an individual will not have access to the notice.

9. Notification and Redress

a. What are the procedures to allow individuals to gain access to their information and to amend information they believe to be incorrect?

Procedures for notification and redress are published in the system of records notices identified in paragraph 8 above, and in rules published at 22 CFR 171.3. The procedures inform the individual about how to inquire about the existence of records regarding them, how to request access to their records, and how to request an amendment of their records. Certain exemptions to Privacy Act provisions for notification and redress may exist for certain portions of passport records on grounds pertaining to law enforcement in the interest of national defense and foreign policy, if the records have been properly classified, and to carry out protective responsibilities under 18 U.S.C. 3056. These exemptions are published as agency rules at 22 CFR 171.36.

b. Privacy Impact Analysis: Discuss the privacy risks associated with notification and redress and how those risks are mitigated.

The risk of notification and redress is mitigated by the publication of the System of Records notices in the *Federal Register* and on the State Department webpage*.*

10. Controls on Access

a. What procedures are in place to determine which users may access the system and the extent of their access? What monitoring, recording, and auditing safeguards are in place to prevent misuse of data?

Authorized VRS users' access is limited to the five user function levels (0-4). These levels allow VRS to comply with least privilege and accurately keep track of each user's actions within the VRS database server. They also protect the user from having data entered or modified by someone else under the user's identity. Database administrators authenticate to and are authorized by the Oracle server application. Authorized users must first authenticate to OpenNet using their user ID and password and this information is used to authenticate against the VRS user table for a matching account.

VRS supports six user groups: VRS specialists, managers, couriers, office clerks (for express mail), system administrators, and database administrators. The VRS admin guide lists the permissions that go with each user level. The user interface and the database both automatically enforce user permissions. Assignment of permissions is done manually by level 3 and 4 users. Level 3 users cannot assign level 4 permissions.

All VRS users, including system administrators, receive their access through local access requesting procedures organic to the CA organization and compliant with 12 FAM policies. Each user must submit an account request form indicating the requirement for system administrator privileges. The account request is reviewed by the user’s supervisor and must be approved by the VRS system manager before the request can be granted.

VRS employs automated mechanisms to audit account creation, modification, disabling, and termination actions and to notify, as required, appropriate individuals. The auditing reports are generated and reviewed by the database administrator. A subset of audit records, for request history, is available to level 1 users and above via the Trace report, and on the History screen. These reports allow users to view all events that happened to an individual visa request record.

b. What privacy orientation or training for the system is provided to authorized users?

All users are required to undergo computer security and privacy awareness training prior to being given access to the system and must complete refresher training yearly in order to retain access. Upon completion of DS's Security Briefing and CA's in-house Security Awareness presentation, attendees are required to sign forms acknowledging that they have read, understand, and agree to abide by the rules of behavior, before obtaining authorized access to the information system and its resident information. Internet based Visa Request System users will be required to acknowledge reading and accepting the Rules of Behavior before accessing Visa Request System by electronically signing via the Submit button.

c. Privacy Impact Analysis: Given the sensitivity of PII in the system, manner of use, and established access safeguards, describe the expected residual risk related to access.

Privacy vulnerabilities are mitigated by effective administrative procedures for access authorization, account housekeeping, and monitoring, recording, and auditing of user activity. VRS does not use production PII for any reason other than production purposes.

To mitigate the privacy risk from individuals, VRS end-users are required to take DS training for access to OpenNet; media access is also addressed in the Consular Affairs Security Awareness and Training Plan. End users are trained annually with security awareness training to safeguard information system sensitive but unclassified (SBU) data from unauthorized users by storing diskettes, CDs, printouts, etc., in a safe and secure manner. Shredders are provided throughout PPT/SIA for the proper disposal of paper (SBU) medium.

11. Technologies

a. What technologies are used in the system?

VRS operates under standard, commercially-available software products residing on a government-operated computing platform not shared by other business applications or technologies. No technologies commonly considered to elevate privacy risk are used.

VRS is a Government developed product and as such meets required security capabilities, design and development processes, required test and evaluation procedures and documentation under the supervision of its Project Manager in accordance to 5 FAH-5 H-110, Developing and Managing Department of State Projects. All CA/CST contracts have input from DS and CA on security matters in accordance to 12 FAM 650, Acquisition Security Requirements for Operating Systems and Subsystem Components.

Since VRS resides on the OpenNet, it depends on the IDS that are in place for OpenNet to monitor the inbound and outbound communications for unusual or unauthorized activities or conditions. The operating system for VRS is thus configured and maintained according to the State Department's security guidelines and protected by Access Control Lists (ACL).

Additionally, VRS uses the following technologies for their database:

- Oracle Server Logs: archived and moved from the server via Robocopy utility
- VRS Events table: archived via (event records are moved to separate Archive database)

Database Oracle access is restricted by the principle of least privilege via database access controls. No user has direct access to the database; the only means is via the application. For the operating system, it's configured and maintained according to State Dept. security guidelines, and all application files and backups are in locations protected by ACLs.

b. Privacy Impact Analysis: Describe how any technologies used may cause privacy risk, and describe the safeguards implemented to mitigate the risk.

Technologies used are inherently unsecured and, therefore, a security risk from initial implementation. These technology risks, however, are mitigated by VRS's configuration to the correct DS standards and Windows policies created to lock down the system.

12. Security

What is the security certification and accreditation (C&A) status of the system?

The Department operates VRS in accordance with information security requirements and procedures required by federal law and policy to ensure that information is appropriately safeguarded and protected. The Department will conduct a risk assessment of the system to identify appropriate security controls to protect against risk. The Department will perform routine monitoring, testing, and evaluation of security controls to ensure that the controls continue to fully function. In accordance with the Federal Information Security Management Act (FISMA) provision for the triennial recertification of this system, VRS was certified and accredited for 36 months to expire on August 31, 2012. This PIA is being submitted as part of the triennial certification and accreditation process. It is anticipated that the current C&A process will be completed in October 2012 resulting in a projected authorization to operate (ATO) date of October 31, 2015.